Narodowa kryptografia kluczowym elementem systemu bezpieczeństwa państwa [WYWIAD]

8 października 2020, 10:18

Prezes Krypton Michał Czmoch (trzeci od lewej) podczas panelu dyskusyjnego Defence24 DAY, poświęconego cyberbezpieczeństwie i kryptografii. Fot. Kreatyw Media/Defence24.pl.

Andrzej Kozłowski

DOTYCZY:

KRYPTON POLSKA SP. KRYPTOGRAFIA DEFENCE24 DAY PLACÓWKI NAUKOWE NATO ABW SKW MICHAŁ CZMOCH ROBERT KOŚLA MINISTERSTWO CYFRYZACJI

"Każdy suwerenny kraj powinien dążyć do pełnej ochrony najcenniejszych zasobów, jaką jest obecnie informacja. Aby mówić o pełnej ochronie informacji, czyli takiej, do której mamy pewność, że nie może być naruszona, należy mieć własne, krajowe rozwiązania, wytworzone przez własny przemysł, zgodnie z wymaganiami zdefiniowanymi przez służby specjalne. Takie podejście zapewnia pełną kontrolę państwa nad stosowanymi rozwiązaniami

Polityka i Prawo

Armia i Służby

Bezpieczeństwo Informacyjne

Biznes i Finanse

WAŻNE

„Hack dekady" dotknął infrastrukturę krytyczną USA. Co grozi Amerykanom?

Hakerzy wstrzymali dystrybucję gazet w Niemczech

Wirus, wirus wszędzie! Jak dezinformacyjne narracje pokazały nasze słabości?

Amerykańscy urzędnicy nękani groźbami. Irańska reakcja na wynik wyborów prezydenckich?

The best of CyberDefence24 w roku 2020

WIADOMOŚCI

BIZNES I FINANSE
HAKERZY WSTRZYMALI DYSTRYBUCJĘ GAZET W NIEMCZECH

„Zamach na wolny internet". Spór Apple i Facebooka o prywatność użytkowników

Nowości w aplikacji STOP COVID

Jak mądrze i z dystansem budować swoją obecność w mediach społecznościowych?

Włamanie do Europejskiej Agencji Leków mniej poważne niż zakładano

kryptograficznymi" mówi prezes Krypton Polska Michał Czmoch. W wywiadzie prezes mówi także o docelowym modelu współpracy na linii przemysł-administracja państwa oraz roli uczelni.

ZOBACZ TAKŻE

POLITYKA I PRAWO
DEFENCE24 DAY: KRAJOWE FIRMY GWARANTEM SUWERENNOŚCI POLSKI

Panie prezesie, podczas konferencji Defence24 Day poruszaliśmy kwestię znaczenia narodowej kryptografii w budowie systemu bezpieczeństwa państwa. Paneliści byli zgodni co do konieczności rozwoju kompetencji państwa w tym obszarze, w oparciu o krajowe rozwiązania. W tym kontekście mówiliśmy o współpracy polskich firm i instytucji państwa. Wiem, że nie o wszystkich aktualnie realizowanych projektach z tego obszaru możemy dyskutować, ze względu na niejawny charakter programów, zapytam więc bardziej ogólnie: Jakie kompetencje posiadają dzisiaj polskie firmy z obszaru krypto? Czy są w stanie dostarczać kompleksowe rozwiązania dla do instytucji przetwarzających informacje niejawne, czyli istotne dla bezpieczeństwa państwa?

To prawda, narodowa kryptografia jest istotnym elementem kompleksowego systemu bezpieczeństwa państwa. Ośmielę się nawet postawić tezę, że jest jednym z najistotniejszych elementów takiego systemu. Do czego nam bowiem wszystkie systemy obronne, jeśli wróg będzie mógł poznać (podsłuchać) informacje o jego rozlokowaniu i zamiarze użycia? Przyczynia się do ochrony informacji, która zawsze była, a w obecnych czasach jest jeszcze bardziej istotna dla zachowania pokoju lub wygrania starcia Tą informacją może być zarówno pozycja wojsk, dane dotyczące zasobności i lokalizacji źródeł cennych surowców, ale również dane dotyczące bieżących planów gospodarczych rządu czy planów inwestycyjnych spółki giełdowej. Wszystkie te informacje wykradzione i użyte w niewłaściwy sposób mogą wpłyną na destabilizację sytuacji lub nawet wywołanie konfliktu.

Myślę, że paneliści byli zgodni co do konieczności rozwoju kompetencji państwa w tym obszarze w oparciu o krajowe rozwiązania, ponieważ kraj określany mianem niezależnego, niepodległego, a przede wszystkim suwerennego powinien dążyć do pełnej ochrony najcenniejszych zasobów, a tym jak już przed chwilą wspomniałem jest bezsprzecznie informacja. Aby mówić o pełnej ochronie informacji, czyli takiej, do której mamy pewność, że nie może być naruszona, należy mieć własne, krajowe rozwiązania, wytworzone przez własny przemysł, zgodnie z wymaganiami zdefiniowanymi przez służby specjalne. Takie podejście zapewnia pełną kontrolę państwa nad stosowanymi rozwiązaniami kryptograficznymi. W przeciwnym wypadku można mieć tylko nadzieję, że zakupione „z zewnątrz" rozwiązanie kryptograficzne realizuje opisane przez producenta funkcje. Ale takie kwestie jak przesyłanie podprogowe danych, backdoory, cykle generatorów losowych to raczej tematy na seminarium naukowe a nie na dzisiejszy wywiad, dlatego przejdę już do meritum.

ANALIZY

FAKE NEWS
KRÓTKI PRZEWODNIK PO FAKE NEWSACH O KORONAWIRUSIE [AKTUALIZACJA 30.11.2020]

Krótki przewodnik po fake newsach o 5G [Aktualizacja 15.10.2020]

Fundamentalizm na miarę XXI wieku. Internet cichym narzędziem terrorystów

Burza w USA po atakach na rząd. Trump wtóruje Putinowi?

Co zyskuje Orlen przejmując Polska Press?

TWEETS CYBERDEFENCE24

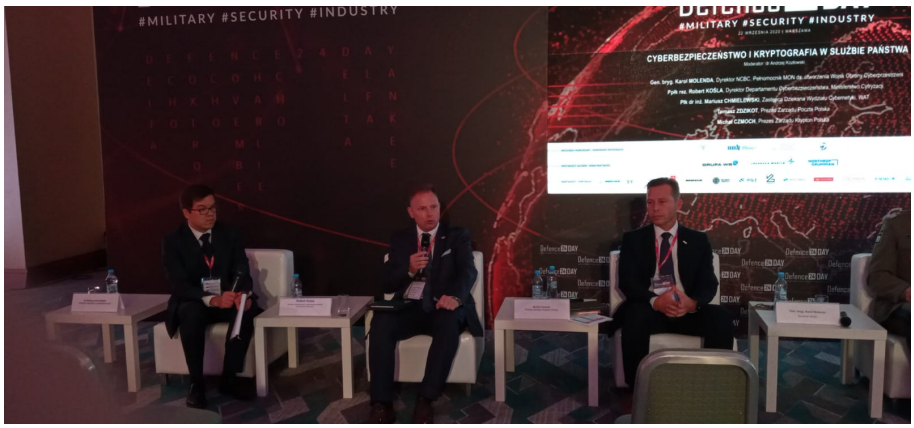
Tweety użytkownika @CyberDefence24

CyberDefence24
@CyberDefence24

Hakerzy zainfekowali co najmniej 15 podmiotów odpowiedzialnych za infrastrukturę krytyczną USA, które korzystały z oprogramowania „Orion". | @Defence24pl @Microsoft @CrowdStrike #HackDekady #Rosja #USA cyberdefence24.pl/hack-dekady-do…

„Hack dekady" dotknął infrastrukturę …
Hakerzy zainfekowali co najmniej kilkana…
cyberdefence24.pl

Umieść Zobacz na Twitterze



Polskie firmy przez wiele lat, a nawet dziesięcioleci rozwijały swoje kompetencje, aby móc spełnić wymagania polskich służb specjalnych. Przez te lata zbudowanych zostało dziesiątki rozwiązań, z których część ma certyfikaty i chroni krajowe systemy po dziś dzień. Są to rozwiązania zgodne nie tylko z naszymi krajowymi wymaganiami, ale co ważne z wymaganiami NATO. Jesteśmy zatem w stanie dostarczać rozwiązania nie tylko na rynek krajowy, ale również NATOwski. To wymaga oczywiście dodatkowych działań po stronie państwa polskiego, ale ja mówię teraz o potencjale i możliwości polskiego przemysłu, który reprezentuje światowy poziom technologii i umiejętności budowy środków ochrony kryptograficznej. I tak jak Pan redaktor wspomniał, nie o wszystkich rozwiązaniach można mówić otwarcie i nie wszystkie są widoczne na oficjalnych listach certyfikatów ABW i SKW. Zapewniam jednak, że polski przemysł (chociażby na przykładzie firmy Krypton Polska) ma kompetencje do budowy rozwiązań od poziomu Zastrzeżone do poziomu Ściśle Tajne.

Czy chodzi tylko o szyfratory, czy także inne urządzenia?

Także inne urządzenia i oprogramowanie. Zgodnie ze sztuką, zabezpieczenie powinno być wielopoziomowe, więc szyfrowanie powinno być realizowane zarówno na warstwie łącza danych i sieciowej (warstwa L2 i L3), jak również na warstwie programowej. Do tego trzeba dodać szyfrowanie przechowywanych danych. Można ogólnie powiedzieć, że to wszystko to są „szyfratory" i każdy z nich powinien dawać największą możliwą pewność skuteczności zabezpieczenia informacji.

Systemy oczywiście składają się z szeregu innych elementów jak np. przełączniki, zapory sieciowe, IDSy (*Intrusion Detection System*), IPSy (*Intrusion Prevention System*), systemy operacyjne, systemy kontroli dostępu, systemy uwierzytelniające itd. Ideałem byłoby mieć własne krajowe rozwiązania (tworzone w modelu o jakim mówiłem na wstępie) i do tego trzeba w miarę możliwości dążyć, aby móc w pełni kontrolować i zapewniać ciągłość usług. Jeżeli jednak mówimy o poufności informacji, to tu kluczowe i krytyczne są środki ochrony kryptograficznej, potocznie nazywane szyfratorami.

Mówi Pan o tym, że polskie firmy mają kompetencje i możliwości nie tylko do produkcji, ale także do projektowania nowych urządzeń kryptograficznych. To duży postęp, jeżeli porównamy możliwości polskiego przemysłu z końca lat 90-tych. Podczas Defence24 Day, Robert Kośla z Ministerstwa Cyfryzacji, mówił o sytuacji sektora przed wejściem Polski do NATO, gdy branża była budowana od zera. Jaka jest zatem dzisiaj kondycja producentów rozwiązań kryptograficznych?

Tak, zgadzam się z tym co mówił Dyrektor Kośla podkreślając postęp jaki polskie firmy osiągnęły w ciągu ostatnich dwóch dekad. Wynika to zarówno z zaangażowania polskiego przemysłu, ale również z pewnej otwartości i zaangażowania jakiego od końca lat 90-tych, doświadczyły firmy od polskich służb specjalnych. Dzięki temu,

powstało szereg polskich rozwiązań. Może nie każde z nich było udane, może nie każde było wówczas na światowym poziomie, ale nie błądzi tylko ten co nic nie robi. Dlatego uważam, że siłą rozwoju polskiego przemysłu jest inicjowanie szeregu projektów, które pozwalają na ciągły rozwój kompetencji.

Budowa rozwiązań kryptograficznych jest bardzo trudnym i złożonym procesem. Dlatego projekty zlecane przez Państwo firmom specjalizującym się w tym zakresie, nie muszą zawsze dotyczyć budowy gotowych, kompletnych systemów. Mogą to być cząstkowe prace, nastawione na badanie kluczowych tematów, które później, zebrane w końcowym projekcie, dadzą pożądany efekt. Niestety, obecnie, takich tematów jest niewiele, a te które są, realizują za własne środki polskie firmy, bez wsparcia Państwa.

Projekty kierowane do przemysłu skupiają się na opracowaniu gotowych rozwiązań, a tych jest niewiele, co dziwi w obliczu rozwoju technologicznego jaki obecnie dzieje się na świecie.

Jest wiele tematów, które wymagają rozpoznania jak np. kryptografia postkwantowa, szybka wymiana algorytmów kryptograficznych, rozwój platform sprzętowych o wysokiej wydajności itd. Te tematy powinny być inicjowane przez służby odpowiedzialne za ochronę kryptograficzną w kraju, zgodnie z opracowaną strategią. Firmy owszem mogą same inwestować w pewne rozwiązania jednak brak wyznaczonego kierunku (poprzez definiowanie tematów) oraz brak współfinansowania (np. w ramach Partnerstwa Prywatno-Publicznego), szybko doprowadzi do recesji technologicznej w tym obszarze. Poniesione straty odrabia się zaś przez dekady.

Dlatego uważam, że siłą rozwoju polskiego przemysłu jest inicjowanie przez Państwo tych wszystkich tematów, które mogą być zrealizowane przez firmy prywatne (póki co wiodące na polskim rynku krypto), co umożliwi im nie tylko ciągły rozwój kompetencji, ale zapewni środki do funkcjonowania. Bez istotnie większej ilości projektów zlecanych przez Państwo, nie osiągnie się zamierzonego celu utrzymania mocnej, narodowej kryptografii.

Jak Pan ocenia współpracę z administracją publiczną w rozwijaniu rozwiązań kryptograficznych? Czy jest różnica we współpracy z cywilnymi instytucjami (służbami) i Siłami Zbrojnymi/MON?

Życzył bym Polsce, aby tej współpracy było więcej, aby więcej tematów trafiało do przemysłu w celu wypracowania nowych rozwiązań zgodnych z ustaloną polityką rozwoju tej dziedziny obronności. Bo tak jak opisałem w odpowiedzi na poprzednie pytanie, ta współpraca przyniosłaby wymierne rezultaty. I nie ważne kto byłby inicjatorem tych tematów - strona cywilna czy wojskowa.

Z instytucjami cywilnymi rozmawia nam się łatwiej, gdyż nie ma tylu „usztywniających", formalnych procedur. Nie jest to jednak tak istotne jak brak tematów (zadań) do realizacji. Krypton Polska realizował projekty zarówno ze służbami cywilnymi jak i MONem i w obu przypadkach odnosiliśmy sukcesy. Mogłyby one może przychodzić szybciej gdyby pewne formuły realizacji uprościć i podchodzić do tematów kryptograficznych (realizowanych z zastosowaniem najnowszych technologii), w sposób bardziej elastyczny, tak jak powinno podchodzić się do projektów informatycznych – np.: sposób realizacji może zmieniać się w trakcie projektu i nie należy tego wstrzymywać; czasami lepiej poświęcić więcej czasu na fazę koncepcyjną niż to wynika z narzuconego harmonogramu; innowacyjne zmiany proponowane przez wykonawcę w trakcie prac projektowych, uznawać jako dodatkowy walor rozwiązania a nie złamanie zapisów umowy.

Warto też zastanowić się nad stosowaniem w odniesieniu do projektów kryptograficznych zasady IIPB, która przyniesie korzyści w postaci szybkiego rozpoczęcia projektu, a nie narzuci mu sztywne formalne wymagania powodujące, iż procedura przygotowania do rozpoczęcia finansowania prac trwa latami.

Podczas Defence24 Day była omawiana kwestia powołania Agencji Uzbrojenia – nowej instytucji, która ma skonsolidować rozproszone dzisiaj kompetencje planistyczne i zakupowe w polskiej armii. Jak Pan ocenia ten pomysł?

Pomysł jest bardzo dobry, ale najważniejsza jest jego realizacja. Jeżeli powołanie Agencji pomoże zlikwidować bolączki, o których mówiłem wcześniej, to będzie milowy krok w rozwoju polskiej armii. Jeśli zaś samo powołanie Agencji skupi się na ustalaniu struktur, procedur, formalizmów i zasad, to będą to kolejne zmarnowane lata.

Jaki, z Pana perspektywy, powinien być docelowy model współpracy pomiędzy przemysłem a sektorem publicznym w obszarze rozwoju zagadnień kryptograficznych? Co jest konieczne, żeby programy/projekty realizowane z instytucjami państwa kończyły się powodzeniem?

Podział ról pomiędzy przemysłem, a sektorem publicznym w tym obszarze jest ściśle określony i myślę, że nie ma potrzeby go zmieniać. Służby definiują wymagania, opracowują samodzielnie (lub przy wsparciu przemysłu) kluczowe elementy sytemu kryptograficznego, jak np. algorytmy, mechanizmy ich wymiany i generacji materiału kryptograficznego. Następnie zlecają wykonanie przez przemysł konkretnych rozwiązań technicznych o określonych parametrach (ale takich realnych i dostosowanych do możliwości technologicznych na świecie), a następnie po wykonaniu tych prac badają (certyfikują) wytworzone przez przemysł rozwiązanie i implementują tam narodową kryptografię. Taki sposób postępowania obowiązuje we wszystkich znanych mi krajach posiadających silne rozwiązania kryptograficzne. Przemysł sam poradzi sobie z rozbudową wymaganych kompetencji, jeśli tylko będzie miał cel i fundusze by to robić – czyli jeśli będą powoływane projekty, które będą zmierzały do budowy zaawansowanych rozwiązań kryptograficznych. Firmy prywatne nie są w stanie samodzielnie finansować budowy (rozwoju) tak skomplikowanej dziedziny jaką jest narodowa kryptografia. Nikt nie będzie rozbudowywał własnych kompetencji „dla sportu", tylko dlatego, że może kiedyś się komuś to przyda.

Tak to wygląda od strony realizacji projektu budowy szyfratora. Ale ważna jest jeszcze formuła dochodzenia do współpracy sektora publicznego z przemysłem i osobiście nie uważam, że dobrą metodą jest organizacja przetargów, nawet jeśli nie są one organizowane zgodnie z PZP. Formuła przetargu jest dobra na zakup konkretnego produktu istniejącego na rynku (ale i tu czasami przetarg obnaża swoje słabości, jeśli wymagania nie są precyzyjnie i poprawnie zdefiniowane). W przypadku projektów kryptograficznych, gdzie ma dojść do opracowania (często od podstaw) i zbudowania kompletnego, złożonego technologicznie produktu, formuła przetargu moim zdaniem nie powinna mieć zastosowania.

Rozwój polskiej kryptografii nie może odbyć się bez udziału placówek naukowych. Jak powinna wyglądać współpraca przemysłu z uczelniami?

Oczywiście, że polska kryptografia wymaga zaangażowania polskich placówek naukowych. Moim zdaniem to jednak się dzieje. Krypton sam uczestniczył w kilku projektach, w których jednym z konsorcjantów była placówka naukowa. Osobiście bardzo dobrze wspominam tą współpracę, ponieważ w jej efekcie powstały ciekawe

rozwiązania, które mogą obecnie być wykorzystane. Sami też próbowaliśmy inicjować szereg prac badawczo-naukowych z placówkami naukowymi, jednak te od miesięcy czekają na ocenę NCBIR...

Można to podsumować stwierdzeniem, że jak są tematy wymagające nowej myśli naukowej to przemysł i placówki naukowe umieją doskonale się porozumieć w imię opracowania nowych rozwiązań.

Na koniec chciałbym jeszcze podkreślić, że jeśli Polska aspiruje do grona państw posiadających własne rozwiązania kryptograficzne budowane w modelu „Państwo-Przemysł", to bez aktywnego wsparcia przez Państwo firm kryptograficznych nie uda się zbudować narodowej kryptografii, a Polska nie będzie miała możliwości zaistnienia ze swoimi urządzeniami w NATO. Sięganie do firm prywatnych tylko w momencie, gdy w danej chwili potrzebne są nowe rozwiązania kryptograficzne nie sprawdzi się na dłuższą metę.

Czytaj też: Narodowa kryptologia kluczem do suwerenności technologicznej

Andrzej Kozłowski

KOMENTARZE

LICZBA KOMENTARZY: **2**

TREŚĆ KOMENTARZA

AUTOR KOMENTARZA

Autor

123 abc

czwartek, 8 października 2020, 18:26

Kryptografia musi mieć bardzo ważną cechę , bez której trudno o dobre przekazywanie informacji. Musi mieć zaimplementowane elementy charakteryzujące dialog wewnątrz wiadomosci zaszyfrowane innym systemem (na przykład w ramach wiadomości musi

być podana historia wcześniejszych wysłanych i odebranych wiadomości (historia w znaczeniu podanie daty wiadomosci , numer porządkowy ostatniej wiadomości odebranej (zabezpieczy ewentualne zagłuszanie) , numer wiadomości wysłanej). Po co takie coś ? Bez tego wróg może próbować wtrącić się do rozmowy i znając główną metodę szyfracji i deszyfracji łatwo może się podszyć pod jedną ze stron. Brak elementów o historycznych rozmowach wcześniejszych (typu kiedy była ostatnia wiadomość itd) będzie wskazówką na to, że przeciwnik zdołał się wedrzeć do systemu kryptograficznego ale nie udało mu się pobrać (podsłuchać) bazy rozmów.

ODPOWIEDZ

123 abc

czwartek, 8 października 2020, 21:20

Ps. Zdublowanie numeru porządkowego - czyli wiadomość kolejna od rozmówcy - Boba, ale z tym samym numerem porządkowym , to będzie sygnał o wtrąceniu się do rozmowy lub pomyłce. Wtedy trzeba przerwać wymianę informacji danym kanałem (oraz zacząć wysyłać informacje "trashowe" dla niepoznaki) i wyjaśnić skąd zaszła "pomyłka". Jeżeli pomyłka wynika ze zwykłego przeoczenia ostatniej wiadomości to można dalej kontynuować rozmowę. Tutaj uwaga. Rozwianie wątpliwości musi być obowiązkowo innym kanałem , ponieważ wróg Mallory może zagłuszyć Boba i udając roztargnionego podszyć się pod niego uzyskując cenne informacje szpiegowskie.

ODPOWIEDZ

POLITYKA I PRAWO

ARMIA I SŁUŻBY

BEZPIECZEŃSTWO INFORMACYJNE

UNIJNE SANKCJE ZA CYBERATAKI. SUKCES DYPLOMATYCZNY, KTÓRY NIE ZATRZYMA HAKERÓW [KOMENTARZ]

WASZYNGTON OPUBLIKOWAŁ LISTĘ FIRM POWIĄZANYCH Z WOJSKIEM ROSJI I CHIN

WIRUS, WIRUS WSZĘDZIE! JAK DEZINFORMACYJNE NARRACJE POKAZAŁY NASZE SŁABOŚCI?

BIZNES I FINANSE

HAKERZY WSTRZYMALI DYSTRYBUCJĘ GAZET W NIEMCZECH